

Symmetric chains, Gelfand-Tsetlin chains, and the Terwilliger algebra of the binary Hamming scheme

Murali K. Srinivasan

Department of Mathematics

Indian Institute of Technology, Bombay

Powai, Mumbai 400076, INDIA

`mks@math.iitb.ac.in`

Mathematics Subject Classifications: 05A15, 05A30.

To the memory of Mobi

Abstract

The de Bruijn-Tengbergen-Kruyswijk (BTK) construction is a simple algorithm that produces an explicit symmetric chain decomposition of a product of chains. We linearize the BTK algorithm and show that it produces an explicit symmetric Jordan basis (SJB). In the special case of a Boolean algebra the resulting SJB is orthogonal with respect to the standard inner product and, moreover, we can write down an explicit formula for the ratio of the lengths of the successive vectors in these chains (i.e., the singular values). This yields a new, constructive proof of the explicit block diagonalization of the Terwilliger algebra of the binary Hamming scheme. We also give a representation theoretic characterization of this basis that explains its orthogonality, namely, that it is the canonically defined (upto scalars) symmetric Gelfand-Tsetlin basis.

1 Introduction

The de Bruijn-Tengbergen-Kruyswijk (BTK) construction is a simple visual algorithm in matching theory that produces an explicit symmetric chain decomposition of a (finite) product of (finite) linear orders. We show that the BTK algorithm admits a simple and natural linear analog. The main purpose of this paper is to study the linear BTK algorithm as an object in itself. It enables us to explicitly study the up operator (i.e., the nilpotent operator taking an element to the sum of the elements covering it) on a product of linear orders by producing an explicit symmetric Jordan basis (SJB). In the special case of a Boolean algebra the resulting SJB is orthogonal with respect to (wrt) the standard inner product and, moreover, we can write down an explicit formula for the ratio of the lengths of the successive vectors in these chains (i.e., the singular values). This yields a new constructive proof of the explicit block

diagonalization of the Terwilliger algebra of the binary Hamming scheme, recently achieved by Schrijver. We also give a representation theoretic characterization of this basis that explains its orthogonality, namely, that it is the canonically defined (upto scalars) symmetric Gelfand-Tsetlin basis (wrt the up operator on the Boolean algebra).

A (finite) *graded poset* is a (finite) poset P together with a *rank function* $r : P \rightarrow \mathbb{N}$ such that if q covers p in P then $r(q) = r(p) + 1$. The *rank* of P is $r(P) = \max \{r(p) : p \in P\}$ and, for $i = 0, 1, \dots, r(P)$, P_i denotes the set of elements of P of rank i . A *symmetric chain* in a graded poset P is a sequence (p_1, \dots, p_h) of elements of P such that p_i covers p_{i-1} , for $i = 2, \dots, h$, and $r(p_1) + r(p_h) = r(P)$, if $h \geq 2$, or else $2r(p_1) = r(P)$, if $h = 1$. A *symmetric chain decomposition* (SCD) of a graded poset P is a decomposition of P into pairwise disjoint symmetric chains.

We now define the linear analog of a SCD. For a finite set S , let $V(S)$ denote the complex vector space with S as basis. Let P be a graded poset with $n = r(P)$. Then we have $V(P) = V(P_0) \oplus V(P_1) \oplus \dots \oplus V(P_n)$ (vector space direct sum). An element $v \in V(P)$ is *homogeneous* if $v \in V(P_i)$ for some i , and we extend the notion of rank to homogeneous elements by writing $r(v) = i$. A linear map $T : V(P) \rightarrow V(P)$ is said to be *order raising* if, for all $p \in P$, $T(p)$ is a linear combination of the elements covering p (note that this implies that $T(p) = 0$ for all maximal elements of P and that $T(v)$ is homogeneous for homogeneous v). The *up operator* $U : V(P) \rightarrow V(P)$ is defined, for $p \in P$, by $U(p) = \sum_q q$, where the sum is over all q covering p . Let T be an order raising map on a graded poset P . A *graded Jordan chain* in $V(P)$ with respect to T (wrt T for short) is a sequence $v = (v_1, \dots, v_h)$ of nonzero homogeneous elements of $V(P)$ such that $T(v_{i-1}) = v_i$, for $i = 2, \dots, h$, and $T(v_h) = 0$ (note that the elements of this sequence are linearly independent, being nonzero and of different ranks). We say that v *starts* at rank $r(v_1)$ and *ends* at rank $r(v_h)$. If, in addition, v is symmetric, i.e., $r(v_1) + r(v_h) = r(P)$, if $h \geq 2$, or else $2r(v_1) = r(P)$, if $h = 1$, we say that v is a *symmetric Jordan chain*. A *graded Jordan basis* of $V(P)$ wrt T is a basis of $V(P)$ consisting of a disjoint union of graded Jordan chains in $V(P)$ wrt T . If every chain in a graded Jordan basis is symmetric we speak of a *symmetric Jordan basis* (SJB) of $V(P)$ wrt T . When T is the up map U , we drop the “wrt U ” from the notation and speak of a graded Jordan basis/SJB of $V(P)$.

Let n be a positive integer and let k_1, \dots, k_n be nonnegative integers. Define

$$M(n, k_1, \dots, k_n) = \{(x_1, \dots, x_n) \in \mathbb{N}^n : 0 \leq x_i \leq k_i, \text{ for all } i\},$$

and partially order it by componentwise \leq . The cardinality of $M(n, k_1, \dots, k_n)$ is $(k_1 + 1) \dots (k_n + 1)$ and the rank of (x_1, \dots, x_n) is $x_1 + \dots + x_n$, so $r(M(n, k_1, \dots, k_n)) = k_1 + \dots + k_n$. It is easily seen that $M(n, k_1, \dots, k_n)$ is (order) isomorphic to a product of n chains of lengths k_1, \dots, k_n , respectively. Two special cases of $M(n, k_1, \dots, k_n)$ are of interest: the *uniform* case, where $k_1 = \dots = k_n = k$ and we write $M(n, k)$ for $M(n, k, \dots, k)$ and the *Boolean algebra or set* case, where $k_1 = \dots = k_n = 1$ and we write $B(n)$ for $M(n, 1)$.

An algorithm to construct an explicit SCD of $M(n, k_1, \dots, k_n)$ was given by de Bruijn, Tengbergen, and Kruyswijk [BTK, A, E]. We call this the BTK algorithm. Canfield [C], Proctor [P], and Proctor, Saks, and Sturtevant [PSS] proved the existence of a SJB of $V(M(n, k_1, \dots, k_n))$.

These authors work in the more general context of Sperner theory which we do not need here. An overview of this area is given in Chapter 6 of Engel's book [E]. In Section 3 we present a linear analog of the BTK algorithm and prove the following result.

Theorem 1.1 *For a positive integer n and nonnegative integers k_1, \dots, k_n , the linear BTK algorithm constructs an explicit SJB of $V(M(n, k_1, \dots, k_n))$. The vectors in this basis have integral coefficients when expressed in the standard basis $M(n, k_1, \dots, k_n)$.*

When applied to the Boolean algebra $B(n)$ the linear BTK algorithm has properties that go well beyond producing an SJB of $V(B(n))$. We now discuss this. Perhaps the linear BTK algorithm (or a variant) has interesting properties also in the general case but we are unable to say anything on this point here.

When the linear BTK algorithm is run on $B(n)$, the resulting SJB's are all orthogonal wrt the standard inner product on $B(n)$. Moreover, any two symmetric Jordan chains starting at rank k and ending at rank $n - k$ "look alike" in the sense made precise in the following result. Let \langle, \rangle denote the standard inner product on $V(B(n))$, i.e., $\langle X, Y \rangle = \delta(X, Y)$, (Kronecker delta) for $X, Y \in B(n)$. The length $\sqrt{\langle v, v \rangle}$ of $v \in V(B(n))$ is denoted $\|v\|$. The following result is proved in Section 3. (In the formulation below item (ii) is clearly implied by item (iii) but for convenience of later reference we have spelt out item (ii) explicitly.)

Theorem 1.2 *Let $O(n)$ be the SJB produced by the linear BTK algorithm when applied to $B(n)$.*

- (i) *The elements of $O(n)$ are orthogonal with respect to \langle, \rangle .*
- (ii) *Let $0 \leq k \leq \lfloor n/2 \rfloor$ and let (x_k, \dots, x_{n-k}) and (y_k, \dots, y_{n-k}) be any two symmetric Jordan chains in $O(n)$ starting at rank k and ending at rank $n - k$. Then*

$$\frac{\|x_{u+1}\|}{\|x_u\|} = \frac{\|y_{u+1}\|}{\|y_u\|}, \quad k \leq u < n - k.$$

- (iii) *In the notation of part (ii) we have, for $k \leq u < n - k$,*

$$\frac{\|x_{u+1}\|}{\|x_u\|} = \sqrt{(u+1-k)(n-k-u)} \tag{1}$$

$$= (n-k-u) \binom{n-2k}{u-k}^{\frac{1}{2}} \binom{n-2k}{u+1-k}^{-\frac{1}{2}}. \tag{2}$$

In a recent breakthrough, Schrijver [S] obtained new polynomial time computable upper bounds on binary code size using semidefinite programming and the Terwilliger algebra (this approach was later extended to nonbinary codes in [GST]). There are two main steps involved here. The first is to (upper) bound binary code size by the optimal value of an exponential size semidefinite program and the second is to reduce the semidefinite program to polynomial size by explicitly block diagonalizing the Terwilliger algebra. For background on coding theory we refer to [GST, S]. In this paper we consider the second step. Theorem 1.2 contains

most of the information necessary to explicitly block diagonalize the Terwilliger algebra of the binary Hamming scheme. We show this in Section 2. Here we would like to add a few remarks about the present proof of explicit block diagonalization. There are two proofs available for this result: the linear algebraic proof of Schrijver and the representation theoretic proof of Vallentin [V] based on the work of Dunkl [D1, D2]. Our proof can be seen as a constructive version of Schrijver's proof that also has representation theoretic meaning (see Theorem 1.3 below). The basic pattern of the proof is the same as in [S]. Given Theorem 1.2, the rest of the proof is a binomial inversion argument from [S]. On the other hand, though not explicitly stated in this form in [S], the existence of a SJB of $V(B(n))$ satisfying (i), (ii), and (iii) of Theorem 1.2 easily follows from the results in [S]. So the new ingredient here is the explicit construction of the SJB $O(n)$ and its representation theoretic characterization in Theorem 1.3 below. We remark here that this explicit construction is primarily of mathematical interest and is not important from the complexity point of view since even to write down $O(n)$ takes exponential time. We rewrite equation (1) as equation (2) so that the final formula for the block diagonalization turns out to equal Schrijver's which is in a very convenient form with respect to the location of square roots (see Theorem 2.2).

Our proof of Theorem 1.2 is self-contained and elementary but more insight into the result is obtained by using a bit of representation theory. We first give a short proof of existence of a SJB of $V(B(n))$ satisfying (i), (ii), and (iii) of Theorem 1.2 by putting together standard and well-known facts from representation theory.

Define the down operator D on $V(B(n))$ analogous to the up operator and define the operator H on $V(B(n))$ by $H(v_i) = (2i - n)v_i$, $v_i \in V(B(n)_i)$, $i = 0, 1, \dots, n$. It is easy to check that $[H, U] = 2U$, $[H, D] = -2D$, and $[U, D] = H$. Thus the linear map $\mathfrak{sl}(2, \mathbb{C}) \rightarrow \mathfrak{gl}(V(B(n)))$ given by

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \mapsto U, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \mapsto D, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mapsto H$$

is a representation of $\mathfrak{sl}(2, \mathbb{C})$. Decompose $V(B(n))$ into irreducible $\mathfrak{sl}(2, \mathbb{C})$ -submodules and let W be an irreducible in this decomposition with dimension $l + 1$. It follows from the representation theory of $\mathfrak{sl}(2, \mathbb{C})$ (see Section 2.3.1 in [GW]) that there exists a basis $\{v_0, v_1, \dots, v_l\}$ of W such that, for $i = 0, 1, \dots, l$, we have (below we take $v_{-1} = v_{l+1} = 0$)

$$U(v_i) = v_{i+1}, \quad D(v_i) = i(l - i + 1)v_{i-1}, \quad H(v_i) = (2i - l)v_i \quad (3)$$

So the eigenvalues of H on v_0, v_1, \dots, v_l are, respectively, $-l, -l + 2, \dots, l - 2, l$. It now follows from the definition of H that each v_i is homogeneous and that (v_0, \dots, v_l) is a symmetric Jordan chain in $V(B(n))$. Thus there exists a SJB of $V(B(n))$. Note also that the basis $\{v_0, \dots, v_l\}$ of W is canonically determined (upto a common scalar multiple) since the eigenvalues of the v_i on H are distinct. Let $r(v_0) = k$ and put $x_j = v_{j-k}$, $k \leq j \leq n - k$. The symmetric Jordan chain (v_0, \dots, v_l) now gets rewritten as (x_k, \dots, x_{n-k}) and (3) becomes, for $k \leq u \leq n - k$,

$$U(x_u) = x_{u+1}, \quad D(x_u) = (u - k)(n - k - u + 1)x_{u-1}. \quad (4)$$

Now we use the substitution action of the symmetric group S_n on $B(n)$. As is easily seen the existence of a SJB of $V(B(n))$ satisfying (i) and (ii) of Theorem 1.2 follows from the following facts by an application of Schur's lemma:

- (a) Existence of some SJB of $V(B(n))$.
- (b) U is S_n -linear.
- (c) For $0 \leq k \leq n$, $V(B(n)_k)$ is the sum of $\min \{k, n-k\} + 1$ distinct irreducible S_n -modules (this result is well known).
- (d) For a finite group G , a G -invariant inner product on an irreducible G -module is unique upto scalars.

We now again use the $\mathfrak{sl}(2, \mathbb{C})$ action to prove Theorem 1.2(iii). Let $J(n)$ be a SJB of $V(B(n))$ satisfying parts (i) and (ii) of Theorem 1.2. Normalize $J(n)$ to get an orthonormal basis $J'(n)$ of $V(B(n))$. Let (x_k, \dots, x_{n-k}) , $x_u \in V(B(n)_u)$ for all u , be a symmetric Jordan chain in $J(n)$. Put $x'_u = \frac{x_u}{\|x_u\|}$ and $\alpha_u = \frac{\|x_{u+1}\|}{\|x_u\|}$, $k \leq u \leq n-k$ (we take $x_{k-1} = x_{n-k+1} = 0$). We have, for $k \leq u \leq n-k$,

$$U(x'_u) = \frac{U(x_u)}{\|x_u\|} = \frac{x_{u+1}}{\|x_u\|} = \alpha_u x'_{u+1}. \quad (5)$$

Now observe that the matrices, in the standard basis, of U and D are real and transposes of each other. Since $J'(n)$ is orthonormal wrt the standard inner product, it follows that the matrices of U and D , in the basis $J'(n)$, must be adjoints of each other. Thus we must have, using (5), $D(x'_{u+1}) = \alpha_u x'_u$. So the subspace spanned by $\{x_k, \dots, x_{n-k}\}$ is an irreducible $\mathfrak{sl}(2, \mathbb{C})$ -module and formula (4) applies. We have

$$DU(x'_u) = \alpha_u^2 x'_u = (u+1-k)(n-k-u)x'_u$$

and thus $\alpha_u = \sqrt{(u+1-k)(n-k-u)}$.

Using a little bit more representation theory we can give a characterization of $O(n)$ among all SJB's satisfying Theorem 1.2. Consider an irreducible S_n -module V . By the branching rule the decomposition of V into irreducible S_{n-1} -modules is multiplicity free and is therefore canonical. Each of these modules, in turn, decompose canonically into irreducible S_{n-2} -modules. Iterating this construction we get a canonical decomposition of V into irreducible S_1 -modules, i.e., one dimensional subspaces. Thus, there is a canonical basis of V , determined upto scalars, and called the *Gelfand-Tsetlin or Young basis (GZ-basis)* (see [VO]). Note that the GZ-basis is orthogonal wrt the (unique upto scalars) S_n -invariant inner product on V . We now observe the following:

- (i) If $f : V \rightarrow W$ is a S_n -linear isomorphism between irreducibles V, W then the GZ-basis of V goes to the GZ-basis of W .
- (ii) Let V be a S_n -module whose decomposition into irreducibles is multiplicity free. By the GZ-basis of V we mean the union of the GZ-bases of the various irreducibles occuring in the (canonical) decomposition of V into irreducibles. Then the GZ-basis of V is orthogonal wrt any S_n -invariant inner product on V .

Now consider the S_n action on $V(B(n))$. Since U is S_n -linear, the action is multiplicity free on $V(B(n)_k)$, for all k , and there exists a SJB of $V(B(n))$, it follows from points (i) and (ii) above that there is a canonically defined (upto scalars) orthogonal SJB of $V(B(n))$ that

consists of the union of the GZ-bases of $V(B(n)_k)$, $0 \leq k \leq n$. We call this basis the *symmetric Gelfand-Tsetlin basis* of $V(B(n))$. We prove the following result in Section 4.

Theorem 1.3 *The SJB $O(n)$, produced by the linear BTK algorithm when applied to the Boolean algebra $B(n)$, is the symmetric Gelfand-Tsetlin basis of $V(B(n))$.*

In Example 3.4 in Section 3 we write down the symmetric Gelfand-Tsetlin bases of $V(B(n))$ for $n = 1, 2, 3, 4$.

2 Terwilliger algebra of the binary Hamming scheme

The *Terwilliger algebra of the binary Hamming scheme*, denoted \mathcal{T}_n , is defined to be the commutant of the S_n action on $B(n)$, i.e., $\mathcal{T}_n = \text{End}_{S_n}(V(B(n)))$ (in this definition the order structure on $B(n)$ is irrelevant). In this section we explicitly block diagonalize \mathcal{T}_n . It is convenient to think of $B(n)$ as the poset of subsets of the set $\{1, 2, \dots, n\}$.

Being the commutant of a finite group action \mathcal{T}_n is a C^* -algebra. Note that \mathcal{T}_n is noncommutative (since, for example, the trivial representation occurs at every rank and thus more than once). Let us first describe \mathcal{T}_n in matrix terms. We represent elements of $\text{End}(V(B(n)))$ (in the standard basis) as $B(n) \times B(n)$ matrices (we think of elements of $V(B(n))$ as column vectors with coordinates indexed by $B(n)$). For $X, Y \in B(n)$, the entry in row X , column Y of a matrix M will be denoted $M(X, Y)$. The matrix corresponding to $f \in \text{End}(V(B(n)))$ is denoted M_f .

Lemma 2.1 *Let $f : V(B(n)) \rightarrow V(B(n))$ be a linear map. Then f is S_n -linear if and only if*

$$M_f(X, Y) = M_f(\pi(X), \pi(Y)), \text{ for all } X, Y \in B(n), \pi \in S_n.$$

Proof (only if) For $Y \in B(n)$ we have $f(Y) = \sum_{X \in B(n)} M_f(X, Y)X$. Since f is S_n -linear we now have, for $\pi \in S_n$,

$$\sum_{X \in B(n)} M_f(X, \pi(Y))X = f(\pi(Y)) = \pi(f(Y)) = \sum_{X \in B(n)} M_f(X, Y)\pi(X).$$

It follows that $M_f(X, \pi(Y)) = M_f(\pi^{-1}(X), Y)$. Thus we have $M_f(\pi(X), \pi(Y)) = M_f(X, Y)$.

(if) Similar to the only if part. \square

Define \mathcal{A}_n to be the set of all $B(n) \times B(n)$ complex matrices M satisfying $M(X, Y) = M(\pi(X), \pi(Y))$, for all $X, Y \in B(n)$, $\pi \in S_n$. It follows from Lemma 2.1 that \mathcal{A}_n is a C^* -algebra of matrices isomorphic to \mathcal{T}_n . We can easily determine its dimension. For nonnegative integers i, j, t let $M_{i,j}^t$ be the $B(n) \times B(n)$ matrix given by

$$M_{i,j}^t(X, Y) = \begin{cases} 1 & \text{if } |X| = i, |Y| = j, |X \cap Y| = t \\ 0 & \text{otherwise} \end{cases}$$

Given $(X, Y), (X', Y') \in B(n) \times B(n)$, there exists $\pi \in S_n$ with $\pi(X) = X'$, $\pi(Y) = Y'$ if and only if $|X| = |X'|$, $|Y| = |Y'|$, and $|X \cap Y| = |X' \cap Y'|$. It follows that

$$\{M_{i,j}^t \mid i - t + t + j - t \leq n, i - t, t, j - t \geq 0\}$$

is a basis of \mathcal{A}_n and its cardinality is $\binom{n+3}{3}$.

It follows from general C^* -algebra theory that there exists a *block diagonalization* of \mathcal{A}_n , i.e., there exists a $B(n) \times S$ unitary matrix $N(n)$, for some index set S of cardinality 2^n , and positive integers $p_0, q_0, \dots, p_m, q_m$ such that $N(n)^* \mathcal{A}_n N(n)$ is equal to the set of all $S \times S$ block-diagonal matrices

$$\begin{pmatrix} C_0 & 0 & \dots & 0 \\ 0 & C_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_m \end{pmatrix} \quad (6)$$

where each C_k is a block-diagonal matrix with q_k repeated, identical blocks of order p_k

$$C_k = \begin{pmatrix} B_k & 0 & \dots & 0 \\ 0 & B_k & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B_k \end{pmatrix} \quad (7)$$

Thus $p_0^2 + \dots + p_m^2 = \dim(\mathcal{A}_n)$ and $p_0 q_0 + \dots + p_m q_m = 2^n$. The numbers $p_0, q_0, \dots, p_m, q_m$ and m are uniquely determined (upto permutation of the indices) by \mathcal{A}_n .

By dropping duplicate blocks we get a positive semidefiniteness preserving C^* -algebra isomorphism (below $\text{Mat}(n \times n)$ denotes the algebra of complex $n \times n$ matrices)

$$\Phi : \mathcal{A}_n \cong \bigoplus_{k=0}^m \text{Mat}(p_k \times p_k).$$

In an *explicit block diagonalization* we need to know this isomorphism explicitly, i.e., we need to know the entries in the image of $M_{i,j}^t$. In [S], an explicit block diagonalization was determined. We now show that this result follows from Theorem 1.2. The present proof also yields an explicit, canonical (real) unitary matrix $N(n)$ achieving the isomorphism Φ .

The first step is a binomial inversion argument. Fix $i, j \in \{0, \dots, n\}$. Then we have

$$M_{i,t}^t M_{t,j}^t = \sum_{u=0}^n \binom{u}{t} M_{i,j}^u, \quad t = 0, \dots, n,$$

since the entry of the lhs in row X , col Y with $|X| = i, |Y| = j$ is equal to the number of common subsets of X and Y of size t . Apply binomial inversion to get

$$M_{i,j}^t = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} M_{i,u}^u M_{u,j}^u, \quad t = 0, \dots, n. \quad (8)$$

Since $M_{u,j}^u = (M_{j,u}^u)^t$ and it will turn out that $N(n)$ can be taken to be real (see the definition below) it follows that

$$\Phi(M_{i,j}^t) = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} \Phi(M_{i,u}^u) \Phi(M_{j,u}^u)^t, \quad t = 0, \dots, n, \quad (9)$$

and hence all the images under Φ can be calculated by knowing the images $\Phi(M_{i,u}^u)$.

For the second step we use Theorem 1.2 whose notation we preserve. For the rest of this section set $m = \lfloor n/2 \rfloor$, and $p_k = n - 2k + 1$, $q_k = \binom{n}{k} - \binom{n}{k-1}$, $k = 0, \dots, m$. Note that

$$\sum_{k=0}^m p_k^2 = \binom{n+3}{3}, \quad (10)$$

since both sides are polynomials in l (treating the cases $n = 2l$ and $n = 2l + 1$ separately) of degree 3 and agree for $l = 0, 1, 2, 3$.

For $0 \leq k \leq m$, $O(n)$ will contain q_k symmetric Jordan chains, each containing p_k vectors, starting at rank k and ending at rank $n - k$. We can formalize this as follows: define the finite set $S = \{(k, b, i) \mid 0 \leq k \leq m, 1 \leq b \leq q_k, k \leq i \leq n - k\}$. For each $0 \leq k \leq m$, fix some linear ordering of the q_k Jordan chains of $O(n)$ going from rank k to rank $n - k$. Then there is a bijection $\mathcal{B} : O(n) \rightarrow S$ defined as follows: let $v \in O(n)$. Then $\mathcal{B}(v) = (k, b, i)$, where $i = r(v)$ and v occurs on the b th symmetric Jordan chain going from rank k to rank $n - k$ (there are unique such k, b). Linearly order S as follows: $(k, b, i) <_\ell (k', b', i')$ iff $k < k'$ or $k = k', b < b'$ or $k = k', b = b', i < i'$. Form a $B(n) \times S$ matrix $N(n)$ as follows: the columns of $N(n)$ are the normalized images $\frac{\mathcal{B}^{-1}(s)}{\|\mathcal{B}^{-1}(s)\|}$, $s \in S$ listed in increasing order (of $<_\ell$). By Theorem 1.2(i), $N(n)$ is unitary. Since the action of $M_{i,u}^u$ on $V(B(n)_u)$ is $\frac{1}{(i-u)!}$ times the action of U^{i-u} on $V(B(n)_u)$, it follows by Theorem 1.2(ii) and identities (8), (10) above that conjugating by $N(n)$ provides a block diagonalization of \mathcal{A}_n of the form (6), (7) above. Set Φ equal to conjugation by $N(n)$ followed by dropping duplicate blocks. To calculate the images under Φ we shall now use part (iii) of Theorem 1.2.

For $i, j, k, t \in \{0, \dots, n\}$ define

$$\beta_{i,j,k}^t = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} \binom{n-2k}{u-k} \binom{n-k-u}{i-u} \binom{n-k-u}{j-u}.$$

For $0 \leq k \leq m$ and $k \leq i, j \leq n - k$, define $E_{i,j,k}$ to be the $p_k \times p_k$ matrix, with rows and columns indexed by $\{k, k+1, \dots, n-k\}$, and with entry in row i and column j equal to 1 and all other entries 0.

Theorem 2.2 (Schrijver [S]) *Let $i, j, t \in \{0, \dots, n\}$. Write*

$$\Phi(M_{i,j}^t) = (N_0, \dots, N_m),$$

where, for $k = 0, \dots, m$, the rows and columns of N_k are indexed by $\{k, k+1, \dots, n-k\}$. Then, for $0 \leq k \leq m$,

$$N_k = \begin{cases} \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \beta_{i,j,k}^t E_{i,j,k} & \text{if } k \leq i, j \leq n-k \\ 0 & \text{otherwise} \end{cases}$$

Proof Fix $0 \leq k \leq m$. If both i, j are not elements of $\{k, \dots, n-k\}$ then clearly $N_k = 0$. So we may assume $k \leq i, j \leq n-k$. Clearly, $N_k = \lambda E_{i,j,k}$ for some λ . We now find $\lambda = N_k(i, j)$.

Let $u \in \{0, \dots, n\}$. Write $\Phi(M_{i,u}^u) = (A_0^u, \dots, A_m^u)$. We claim that

$$A_k^u = \begin{cases} \binom{n-k-u}{i-u} \binom{n-2k}{u-k}^{\frac{1}{2}} \binom{n-2k}{i-k}^{-\frac{1}{2}} E_{i,u,k} & \text{if } k \leq u \leq n-k \\ 0 & \text{otherwise} \end{cases}$$

The otherwise part of the claim is clear. If $k \leq u \leq n-k$ and $i < u$ then we have $A_k^u = 0$. This also follows from the rhs since the binomial coefficient $\binom{a}{b}$ is 0 for $b < 0$. So we may assume that $k \leq u \leq n-k$ and $i \geq u$. Clearly, in this case we have $A_k^u = \alpha E_{i,u,k}$, for some α . We now determine $\alpha = A_k^u(i, u)$. We have using Theorem 1.2(iii)

$$A_k^u(i, u) = \frac{\prod_{w=u}^{i-1} \left\{ (n-k-w) \binom{n-2k}{w-k}^{\frac{1}{2}} \binom{n-2k}{w+1-k}^{-\frac{1}{2}} \right\}}{(i-u)!} = \binom{n-k-u}{i-u} \binom{n-2k}{u-k}^{\frac{1}{2}} \binom{n-2k}{i-k}^{-\frac{1}{2}}$$

Similarly, if we write $\Phi(M_{u,j}^u) = (B_0^u, \dots, B_m^u)$ then, since $M_{u,j}^u = (M_{j,u}^u)^t$, we have

$$B_k^u = \begin{cases} \binom{n-k-u}{j-u} \binom{n-2k}{u-k}^{\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} E_{u,j,k} & \text{if } k \leq u \leq n-k \\ 0 & \text{otherwise} \end{cases}$$

It now follows from (8) that $N_k = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} A_k^u B_k^u = \sum_{u=k}^{n-k} (-1)^{u-t} \binom{u}{t} A_k^u B_k^u$. Thus

$$\begin{aligned} N_k(i, j) &= \sum_{u=k}^{n-k} (-1)^{u-t} \binom{u}{t} \left\{ \sum_{l=k}^{n-k} A_k^u(i, l) B_k^u(l, j) \right\} \\ &= \sum_{u=k}^{n-k} (-1)^{u-t} \binom{u}{t} A_k^u(i, u) B_k^u(u, j) \\ &= \sum_{u=k}^{n-k} (-1)^{u-t} \binom{u}{t} \binom{n-k-u}{i-u} \binom{n-2k}{u-k}^{\frac{1}{2}} \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-k-u}{j-u} \binom{n-2k}{u-k}^{\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \\ &= \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \left\{ \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} \binom{n-k-u}{i-u} \binom{n-k-u}{j-u} \binom{n-2k}{u-k} \right\}. \end{aligned}$$

3 The linear BTK algorithm

In this section we present the linear analog of the BTK algorithm for constructing a SJB of $V(M(n, k_1, \dots, k_n))$. Though we do not recall here the BTK algorithm for constructing a SCD

of $M(n, k_1, \dots, k_n)$ (see [BTK, A, E]), readers familiar with that method will easily recognize the present algorithm as its linear analog.

The basic building block of the linear BTK algorithm is an inductive method for constructing a SJB of $V(M(2, p, q))$. If p or $q = 0$, then $M(2, p, q)$ is order isomorphic to a chain and the characteristic vectors of the elements of the chain form a SJB. For positive p, q we shall now reduce the problem of constructing a SJB of $V(M(2, p, q))$ to that of constructing a SJB of $V(M(2, p-1, q-1))$. We begin with the following elementary lemma on determinants.

Lemma 3.1 *Let $N = (a_{i,j})$ be a $n \times n$ real matrix, $n \geq 2$. Suppose that*

(i) $a_{i,1} > 0$, for $i \in \{1, \dots, n\}$, i.e., the first column contains positive entries.

(ii) For $j \in \{2, \dots, n\}$, $a_{j,j} > 0$, $a_{j-1,j} < 0$, and all other entries in column j are 0.

Then $\det(N) > 0$.

Proof By induction on n . The assertion is clear for $n = 2$. Now assume that $n > 2$. Let $N[i, j]$ denote the $(n-1) \times (n-1)$ matrix obtained from N by deleting row i and column j . Expanding $\det(N)$ by the first row we get

$$\det(N) = a_{1,1}\det(N[1, 1]) - a_{1,2}\det(N[1, 2])$$

Now $a_{1,1} > 0$, $a_{1,2} < 0$, $N[1, 1]$ is upper triangular with positive diagonal entries, and $\det(N[1, 2]) > 0$ (by induction hypothesis). The result follows. \square

Let p, q be positive and set $P = M(2, p, q)$, $W = V(P)$ with up operator U . Let r denote the rank function of P . We have $\dim W = (p+1)(q+1)$. The action of U on the standard basis of W is given as follows: for $0 \leq i \leq p$, $0 \leq j \leq q$

$$U((i, j)) = \begin{cases} (i+1, j) + (i, j+1) & \text{if } i < p, j < q \\ (i+1, j) & \text{if } i < p, j = q \\ (i, j+1) & \text{if } i = p, j < q \\ 0 & \text{if } i = p, j = q \end{cases}$$

Consider the following symmetric Jordan chain in W generated by $v(0) = (0, 0)$:

$$(v(0), v(1), v(2), \dots, v(p+q)),$$

where, for $0 \leq k \leq p+q$,

$$v(k) = U^k((0, 0)) = \sum_{i,j} \binom{k}{i} (i, j), \quad (11)$$

the sum being over all $0 \leq i \leq p$, $0 \leq j \leq q$ with $i+j = k$.

The following result is basic to our inductive approach.

Theorem 3.2 *Define homogeneous vectors in W as follows:*

$$v(i, j) = (p-i)(i, j) - (q-j+1)(i+1, j-1), \quad 0 \leq i \leq p-1, \quad 1 \leq j \leq q. \quad (12)$$

Then

- (i) $v(i, j)$ is nonzero and $r(v(i, j)) = i + j$, $0 \leq i \leq p - 1$, $1 \leq j \leq q$.
- (ii) $\{v(k) \mid 0 \leq k \leq p + q\} \cup \{v(i, j) \mid 0 \leq i \leq p - 1, 1 \leq j \leq q\}$ is a basis of W .
- (iii) For $0 \leq i \leq p - 1$, $1 \leq j \leq q$ we have

$$U(v(i, j)) = \begin{cases} v(i + 1, j) + v(i, j + 1) & \text{if } i < p - 1, j < q \\ v(i + 1, j) & \text{if } i < p - 1, j = q \\ v(i, j + 1) & \text{if } i = p - 1, j < q \\ 0 & \text{if } i = p - 1, j = q \end{cases}$$

Thus, the action of U on the $v(i, j)$ is isomorphic to the action of the up operator on the standard basis of $V(M(2, p - 1, q - 1))$, except that the map $(i, j) \mapsto v(i, j + 1)$, $(i, j) \in M(2, p - 1, q - 1)$ shifts ranks by one (since $r(v(i, j + 1)) = i + j + 1$).

Proof (i) This is clear.

(ii) For $0 \leq k \leq p + q$ define

$$X_k = \{v(k)\} \cup \{v(i, j) : 0 \leq i \leq p - 1, 1 \leq j \leq q, i + j = k\}$$

The map $\phi_k : X_k \rightarrow M(2, p, q)_k$ given by $\phi_k(v(i, j)) = (i, j)$ and

$$\phi_k(v(k)) = \begin{cases} (k, 0) & \text{if } k < p \\ (p, k - p) & \text{if } k \geq p \end{cases}$$

is clearly a bijection. It is enough to show that X_k is a basis of $V(M(2, p, q)_k)$. Linearly order the elements of $M(2, p, q)_k$ using reverse lexicographic order $<_r$: $(i, j) <_r (i', j')$ if and only if $i > i'$. Transfer this order to X_k via ϕ_k^{-1} . Consider the $M(2, p, q)_k \times X_k$ matrix N , with rows and columns listed in the order $<_r$, and whose columns are the coordinate vectors of elements of X_k in the standard basis $M(2, p, q)_k$ of $V(M(2, p, q)_k)$. Equation (11) shows that hypothesis (i) of Lemma 3.1 is satisfied and equation (12) shows that hypothesis (ii) of Lemma 3.1 is satisfied. The result now follows from Lemma 3.1.

(iii) We check the first case. The other cases are similar. Let $i < p - 1, j < q$. Then

$$\begin{aligned} U(v(i, j)) &= U((p - i)(i, j) - (q - j + 1)(i + 1, j - 1)) \\ &= (p - i)((i + 1, j) + (i, j + 1)) - (q - j + 1)((i + 2, j - 1) + (i + 1, j)) \\ &= (p - i - 1)(i + 1, j) - (q - j + 1)(i + 2, j - 1) + (p - i)(i, j + 1) - (q - j)(i + 1, j) \\ &= v(i + 1, j) + v(i, j + 1), \end{aligned}$$

completing the proof. \square

Theorem 3.2, whose notation we preserve, gives the following inductive method for constructing a SJB of $V(M(2, p, q))$: if p or q equals 0, the chain $M(2, p, q)$ itself gives a SJB. Now suppose $p, q > 1$. Set $v(0) = (0, 0)$ and form the symmetric Jordan chain $C = (v(0), v(1), \dots, v(p + q))$,

where $v(k)$ is given by (11). Take the (inductively constructed) SJB of $V(M(2, p-1, q-1))$ and (using parts (ii) and (iii) of Theorem 3.2) transfer each Jordan chain in this SJB to a Jordan chain in $V(M(2, p, q))$ via the map $(i, j) \mapsto v(i, j+1)$. Since $r(v(0, 1)) = 1$ and $r(v(p-1, q)) = p+q-1$, each such transferred Jordan chain is symmetric in $V(M(2, p, q))$ and part (ii) of Theorem 3.2 now shows that the collection of these chains together with C gives a SJB of $V(M(2, p, q))$.

Example 3.3 (i) Here we work out the SJB of $V(M(2, 2, 2))$ produced by the algorithm above. The symmetric Jordan chain generated by $(0, 0)$ is given by

$$((0, 0), (1, 0) + (0, 1), (2, 0) + 2(1, 1) + (0, 2), 3(2, 1) + 3(1, 2), 6(2, 2)). \quad (13)$$

The $v(i, j)$ are given by

$$\begin{aligned} v(0, 1) &= 2(0, 1) - 2(1, 0) & v(1, 1) &= (1, 1) - 2(2, 0) \\ v(0, 2) &= 2(0, 2) - (1, 1) & v(1, 2) &= (1, 2) - (2, 1) \end{aligned}$$

The SJB of $V(M(2, 1, 1))$ is given by the following two chains

$$\begin{aligned} &((0, 0), (1, 0) + (0, 1), 2(1, 1)) \\ &((0, 1) - (1, 0)) \end{aligned}$$

Transferring these chains to $V(M(2, 2, 2))$ via the map $(i, j) \mapsto v(i, j+1)$ gives the following two chains

$$(v(0, 1), v(1, 1) + v(0, 2), 2v(1, 2)) \quad (14)$$

$$(v(0, 2) - v(1, 1)) \quad (15)$$

Chains (13, 14, 15) give a SJB of $V(M(2, 2, 2))$.

(ii) The procedure above is especially simple when, say $q = 1$, as in this case the recursion stops right at the first stage. For later reference we spell out this case in detail. Consider $M(2, n, 1)$. Define a 1-1 linear map $V(M(2, n, 0)) \rightarrow V(M(2, n, 1))$ by $(i, 0) \mapsto (i, 1)$, $(i, 0) \in M(2, n, 0)$. For $v \in V(M(2, n, 0))$, we denote the image of v under this map by \bar{v} .

Let (x_0, x_1, \dots, x_n) , where $x_i = (i, 0)$ be the SJB of $V(M(2, n, 0))$. Set $x_{-1} = x_{n+1} = 0$. We now consider two cases:

(a) $n = 0$: In this case

$$(x_0, \overline{x_0}). \quad (16)$$

is the SJB of $V(M(2, n, 1))$ produced by Theorem 3.2.

(b) $n \geq 1$: The symmetric Jordan chain in $V(M(2, n, 1))$ generated by $(0, 0)$ can be written as (using (11))

$$(y_0, y_1, \dots, y_{n+1}), \quad \text{where } y_l = x_l + l \overline{x_{l-1}}, \quad 0 \leq l \leq n+1. \quad (17)$$

The SJB of $V(M(2, n, 1))$ produced by Theorem 3.2 is given by (17) and the following symmetric Jordan chain:

$$(z_1, \dots, z_n), \quad \text{where } z_l = (n-l+1) \overline{x_{l-1}} - x_l, \quad 1 \leq l \leq n. \quad (18)$$

We can now give the full linear BTK algorithm which reduces the general case to the $n = 2$ case.

Proof of Theorem 1.1 The proof is by induction on n , the case $n = 1$ being clear and the case $n = 2$ established above. Let $P = M(n, k_1, \dots, k_n)$, $n \geq 3$ and set $V = V(P)$. Denote the rank function of P by r . Define induced subposets $P(j)$ of P by

$$P(j) = \{(a_1, \dots, a_n) \in P : a_n = j\}, \quad 0 \leq j \leq k_n,$$

and set $V(j) = V(P(j))$. Let U denote the up operator on V and U_j denote the up operator on $V(j)$, $0 \leq j \leq k_n$. Note that all the $P(j)$ are order isomorphic. We have

$$V = V(0) \oplus V(1) \oplus \dots \oplus V(k_n). \quad (19)$$

For $0 \leq j < k_n$ define linear isomorphisms $R_j : V(j) \rightarrow V(j+1)$ by

$$R_j((a_1, \dots, a_{n-1}, j)) = (a_1, \dots, a_{n-1}, j+1), \quad (a_1, \dots, a_{n-1}, j) \in P(j)$$

Put $V(k_n + 1) = \{0\}$ and define R_{k_n} to be the zero map.

For $v \in V(j)$, $0 \leq j \leq k_n$ we have

$$U(v) = U_j(v) + R_j(v) \quad (20)$$

$$U_{j+1}R_j(v) = R_jU_j(v) \quad (21)$$

By induction there is a SJB of $V(0)$ (wrt U_0). Let t denote the number of symmetric Jordan chains in this SJB, with the m^{th} chain denoted by

$$S(0, m) = (v(0, 0, m), v(1, 0, m), \dots, v(l_m, 0, m)), \quad 1 \leq m \leq t,$$

where $l_m \geq 0$ is the length of the m^{th} symmetric Jordan chain. Thus

$$\begin{aligned} r(v(0, 0, m)) + r(v(l_m, 0, m)) &= k_1 + \dots + k_{n-1} & \text{if } l_m > 0 \\ 2r(v(0, 0, m)) &= k_1 + \dots + k_{n-1} & \text{if } l_m = 0 \end{aligned}$$

Define subspaces $X(0, m) \subseteq V(0)$ by

$$X(0, m) = \text{Span } S(0, m) = \text{Span } \{v(0, 0, m), \dots, v(l_m, 0, m)\}, \quad 1 \leq m \leq t$$

We have $V(0) = X(0, 1) \oplus \dots \oplus X(0, t)$. Note that $\dim X(0, m) = l_m + 1$.

For $1 \leq m \leq t$, $1 \leq j \leq k_n$, $0 \leq i \leq l_m$ define, by induction on j (starting with $j = 1$),

$$v(i, j, m) = R_{j-1}(v(i, j-1, m)) \quad (22)$$

$$S(j, m) = (v(0, j, m), v(1, j, m), \dots, v(l_m, j, m))$$

$$X(j, m) = \text{Span } S(j, m) = \text{Span } \{v(0, j, m), \dots, v(l_m, j, m)\} \quad (23)$$

Since the R_j , $0 \leq j < k_n$ are isomorphisms we have

$$\{v(0, j, m), \dots, v(l_m, j, m)\} \text{ is independent, } 0 \leq j \leq k_n, 1 \leq m \leq t. \quad (24)$$

$$V(j) = X(j, 1) \oplus X(j, 2) \oplus \dots \oplus X(j, t), \quad 0 \leq j \leq k_n. \quad (25)$$

For $1 \leq m \leq t$, $1 \leq j \leq k_n$ we see from (24) and the following inductive calculation on j (using (21)) that each $S(j, m)$ is a graded Jordan chain in $V(j)$ (below we take $v(l_m + 1, 0, m) = 0$, for all m)

$$\begin{aligned} U_j(v(i, j, m)) &= U_j R_{j-1}(v(i, j-1, m)) \\ &= R_{j-1} U_{j-1}(v(i, j-1, m)) \\ &= R_{j-1}(v(i+1, j-1, m)) \\ &= v(i+1, j, m) \end{aligned} \tag{26}$$

For $m = 1, \dots, t$ define subspaces $Y(m) \subseteq V$ by

$$Y(m) = X(0, m) \oplus X(1, m) \oplus \dots \oplus X(k_n, m). \tag{27}$$

We have from (19) and (25) that

$$V = Y(1) \oplus \dots \oplus Y(t). \tag{28}$$

It follows from (23), (24), and (27) that the set

$$B(m) = \{v(i, j, m) : 0 \leq i \leq l_m, 0 \leq j \leq k_n\}, \quad 1 \leq m \leq t$$

is a basis of $Y(m)$. Note that

$$r(v(i, j, m)) = r(v(0, 0, m)) + i + j, \quad 1 \leq m \leq t, \quad 0 \leq i \leq l_m, \quad 0 \leq j \leq k_n. \tag{29}$$

Fix $1 \leq m \leq t$. Using (20), (22), and (26) we see that the action of U on the basis $B(m)$ is given by

$$U(v(i, j, m)) = \begin{cases} v(i+1, j, m) + v(i, j+1, m) & \text{if } i < l_m, j < k_n \\ v(i+1, j, m) & \text{if } i < l_m, j = k_n \\ v(i, j+1, m) & \text{if } i = l_m, j < k_n \\ 0 & \text{if } i = l_m, j = k_n \end{cases}$$

So this action is isomorphic to the action of the up operator on the standard basis of $V(M(2, l_m, k_n))$, except for the shift of rank given by (29). We can now use the algorithm of Theorem 3.2 to construct an SJB of $Y(m)$ wrt U . Since

$$r(v(0, 0, m)) + r(v(l_m, k_n, m)) = r(v(0, 0, m)) + r(v(l_m, 0, m)) + k_n = k_1 + \dots + k_n,$$

each graded Jordan chain in this SJB is symmetric in V . From (28) it follows that the union of the SJB's of $Y(m)$ gives an SJB of V . That completes the proof. \square

Proof of Theorem 1.2 The proof is by induction of n . The result is clear for $n = 1$. We write $B(n)$ as $M(n, k_1, \dots, k_n)$, where $k_1 = \dots = k_n = 1$.

Consider $V = V(M(n+1, k_1, \dots, k_{n+1}))$, with $k_i = 1$ for all i . We preserve the notation of the proof of Theorem 1.1. Let there be t symmetric Jordan chains in the SJB of $V(0) = V(B(n))$. For $v \in V(0)$, we denote $R_0(v) = \bar{v}$ (agreeing with the notation in Example 3.3(ii)).

We have

$$\begin{aligned} V &= V(0) \oplus V(1) \\ V(0) &= X(0,1) \oplus X(0,2) \oplus \cdots \oplus X(0,t) \\ V(1) &= X(1,1) \oplus X(1,2) \oplus \cdots \oplus X(1,t) \end{aligned}$$

Since the inner product is standard we have

$$\langle u, v \rangle = \langle \overline{u}, \overline{v} \rangle, \quad \langle u, \overline{v} \rangle = 0, \quad u, v \in V(0). \quad (30)$$

It follows that $V(0)$ is orthogonal to $V(1)$. The subspaces $X(0,1), \dots, X(0,t)$ are mutually orthogonal, by the induction hypothesis, and thus

$$V = Y(1) \oplus \cdots \oplus Y(t)$$

is an orthogonal decomposition of V , where

$$Y(m) = X(0,m) \oplus X(1,m), \quad 1 \leq m \leq t.$$

Fix $1 \leq m \leq t$. The subspaces $X(0,m)$ and $X(1,m)$ are orthogonal but Theorem 3.2 will produce new symmetric Jordan chains from linear combinations of vectors in $X(0,m)$ and $X(1,m)$. We now show that these too are orthogonal and satisfy (1). This will prove the theorem.

Write the m^{th} symmetric chain in $V(0)$ as

$$(x_k, \dots, x_{n-k}), \quad 0 \leq k \leq \lfloor n/2 \rfloor, \quad (31)$$

where $r(x_k) = k$. By induction hypothesis

$$\frac{\langle x_{u+1}, x_{u+1} \rangle}{\langle x_u, x_u \rangle} = (u+1-k)(n-k-u), \quad k \leq u < n-k. \quad (32)$$

We now consider two cases.

(a) $k = n - k$: It follows from (16) (after changing n to $n - 2k$ and shifting the rank by k) that the SJB of $Y(m)$ will consist of the single symmetric Jordan chain

$$(x_k, \overline{x_k}). \quad (33)$$

We have

$$\frac{\langle \overline{x_k}, \overline{x_k} \rangle}{\langle x_k, x_k \rangle} = \frac{\langle x_k, x_k \rangle}{\langle x_k, x_k \rangle} = 1 = (k+1-k)(n+1-k-k).$$

(b) $k < n - k$: By (17, 18) the SJB of $Y(m)$ will consist of the following two symmetric Jordan chains (after changing n to $n - 2k$ and shifting the rank by k):

$$(y_k, \dots, y_{n+1-k}), \quad \text{and} \quad (z_{k+1}, \dots, z_{n-k}), \quad (34)$$

where

$$y_l = x_l + (l - k) \overline{x_{l-1}}, \quad k \leq l \leq n + 1 - k. \quad (35)$$

$$z_l = (n - k - l + 1) \overline{x_{l-1}} - x_l, \quad k + 1 \leq l \leq n - k. \quad (36)$$

and $x_{k-1} = x_{n+1-k} = 0$.

For $k + 1 \leq l \leq n - k$ we have from (30)

$$\langle y_l, z_l \rangle = (n - k - l + 1)(l - k) \langle x_{l-1}, x_{l-1} \rangle - \langle x_l, x_l \rangle = 0,$$

where the last step follows from (32) upon substituting $u = l - 1$. Thus

$$\{y_k, \dots, y_{n+1-k}, z_{k+1}, \dots, z_{n-k}\}$$

is an orthogonal basis of $Y(m)$.

We now check (1) for the case $n + 1$. Let $k \leq u < n + 1 - k$. Note that (32) holds for $u = n - k$ also. Also note that in the following computation (in the last but one step) we have used (32) when $u = k - 1$ (in which case the rhs is 0 and the lhs is ∞). This is permissible here because of the presence of the factor $(u - k)^2$.

We have, using (30) and (32),

$$\begin{aligned} \frac{\langle y_{u+1}, y_{u+1} \rangle}{\langle y_u, y_u \rangle} &= \frac{\langle x_{u+1} + (u + 1 - k) \overline{x_u}, x_{u+1} + (u + 1 - k) \overline{x_u} \rangle}{\langle x_u + (u - k) \overline{x_{u-1}}, x_u + (u - k) \overline{x_{u-1}} \rangle} \\ &= \frac{\langle x_{u+1}, x_{u+1} \rangle + (u + 1 - k)^2 \langle x_u, x_u \rangle}{\langle x_u, x_u \rangle + (u - k)^2 \langle x_{u-1}, x_{u-1} \rangle} \\ &= \frac{\frac{\langle x_{u+1}, x_{u+1} \rangle}{\langle x_u, x_u \rangle} + (u + 1 - k)^2}{1 + \frac{\langle x_{u-1}, x_{u-1} \rangle}{\langle x_u, x_u \rangle} (u - k)^2} \\ &= \frac{(u + 1 - k)(n - k - u) + (u + 1 - k)^2}{1 + \frac{(u - k)^2}{(u - k)(n - k - u + 1)}} \\ &= (u + 1 - k)(n + 1 - k - u) \end{aligned}$$

The calculation for $\frac{\langle z_{u+1}, z_{u+1} \rangle}{\langle z_u, z_u \rangle}$ is similar and is omitted. \square

Example 3.4 In this example we work out the SJB's of $V(B(n))$, for $n = 2, 3, 4$, starting with the SJB of $V(B(1))$, using the formulas (31, 33, 34, 35, 36) given in the proof of Theorem 1.2. We write elements of $B(n)$ as subsets of $[n] = \{1, 2, \dots, n\}$ rather than as their characteristic vectors. Thus, for $X \subseteq [n]$, we have $R_0(X) = \overline{X} = X \cup \{n + 1\}$.

(i) The SJB of $V(B(1))$ is given by

$$(\emptyset, \{1\})$$

(ii) The SJB of $V(B(2))$ consists of

$$\begin{aligned} &(\emptyset, \{1\} + \{2\}, 2\{1, 2\}) \\ &(\{2\} - \{1\}) \end{aligned}$$

(iii) The SJB of $V(B(3))$ consists of

$$\begin{aligned} & (\emptyset, \{1\} + \{2\} + \{3\}, 2(\{1, 2\} + \{1, 3\} + \{2, 3\}), 6\{1, 2, 3\}) \\ & (2\{3\} - \{1\} - \{2\}, \{1, 3\} + \{2, 3\} - 2\{1, 2\}) \\ & (\{2\} - \{1\}, \{2, 3\} - \{1, 3\}) \end{aligned}$$

(iv) The SJB of $V(B(4))$ consists of (some of the chains are split across two lines)

$$\begin{aligned} & (\emptyset, \{1\} + \{2\} + \{3\} + \{4\}, 2(\{1, 2\} + \{1, 3\} + \{1, 4\} + \{2, 3\} + \{2, 4\} + \{3, 4\}), \\ & 6(\{1, 2, 3\} + \{1, 2, 4\} + \{1, 3, 4\} + \{2, 3, 4\}), 24\{1, 2, 3, 4\}) \\ & (3\{4\} - (\{1\} + \{2\} + \{3\}), 2(\{1, 4\} + \{2, 4\} + \{3, 4\}) - 2(\{1, 2\} + \{1, 3\} + \{2, 3\}), \\ & 2(\{1, 2, 4\} + \{1, 3, 4\} + \{2, 3, 4\}) - 6\{1, 2, 3\}) \\ & (2\{3\} - (\{1\} + \{2\}), \{1, 3\} + \{2, 3\} - 2\{1, 2\} + 2\{3, 4\} - (\{1, 4\} + \{2, 4\}), \\ & 2(\{1, 3, 4\} + \{2, 3, 4\}) - 4\{1, 2, 4\}) \\ & (\{2\} - \{1\}, \{2, 3\} - \{1, 3\} + \{2, 4\} - \{1, 4\}, 2(\{2, 3, 4\} - \{1, 3, 4\})) \\ & (\{2, 4\} - \{1, 4\} - \{2, 3\} + \{1, 3\}) \\ & (2(\{3, 4\} + \{1, 2\}) - (\{1, 4\} + \{2, 4\} + \{1, 3\} + \{2, 3\})) \end{aligned}$$

It may be verified that each of the SJB's are orthogonal and satisfy (1).

4 Symmetric Gelfand-Tsetlin basis

In this section we prove Theorem 1.3. The proof is an application of the Vershik-Okounkov [VO] theory of (complex) irreducible representations of the symmetric group. We first recall briefly (without proofs) those points of the theory which we need:

(A) A direct elementary argument is given to show that branching from S_n to S_{n-1} is simple, i.e., multiplicity free. Once this is done we have the canonically defined (upto scalars) Gelfand-Tsetlin basis (or GZ-basis) of an irreducible S_n -module, as in the introduction. As stated there, the GZ-basis of an irreducible representation V is orthogonal wrt the unique (upto scalars) S_n -invariant inner product on V .

(B) Denote by S_n^\wedge the set of equivalence classes of finite dimensional complex irreducible representations of S_n . Denote by L^λ the irreducible S_n -module corresponding to $\lambda \in S_n^\wedge$.

We have identified a canonical basis, namely the GZ-basis, in each irreducible representation of S_n . A natural question at this point is to identify those elements of $\mathbb{C}[S_n]$ that act diagonally in this basis (in every irreducible representation). In other words, consider the algebra isomorphism

$$\mathbb{C}[S_n] \cong \bigoplus_{\lambda \in S_n^\wedge} \text{End}(L^\lambda), \quad (37)$$

given by

$$\pi \mapsto (L^\lambda \xrightarrow{\pi} L^\lambda : \lambda \in S_n^\wedge), \quad \pi \in S_n.$$

Let $D(L^\lambda)$ consist of all operators on L^λ diagonal in the GZ-basis of L^λ . The question above can now be stated as: what is the image under the isomorphism (37) of the subalgebra $\bigoplus_{\lambda \in S_n^\wedge} D(L^\lambda)$ of $\bigoplus_{\lambda \in S_n^\wedge} \text{End}(L^\lambda)$.

Let Z_n denote the center of the algebra $\mathbb{C}[S_n]$ and set GZ_n equal to the subalgebra of $\mathbb{C}[S_n]$ generated by $Z_1 \cup Z_2 \cup \dots \cup Z_n$ (where we have the natural inclusions $S_1 \subseteq S_2 \subseteq \dots$). It is easy to see that GZ_n is a commutative subalgebra of $\mathbb{C}[S_n]$. It is called the *Gelfand-Tsetlin algebra* (*GZ-algebra*) of the inductive family of group algebras $\mathbb{C}[S_n]$. It is proved that GZ_n is the image of $\bigoplus_{\lambda \in S_n^\wedge} D(L^\lambda)$ under the isomorphism (37) above, i.e., GZ_n consists of all elements of $\mathbb{C}[S_n]$ that act diagonally in the GZ-basis in every irreducible representation of S_n . Thus GZ_n is a maximal commutative subalgebra of $\mathbb{C}[S_n]$ and its dimension is equal to $\sum_{\lambda \in S_n^\wedge} \dim L^\lambda$. By a GZ-vector v we mean an element of the GZ-basis of L^λ , for some $\lambda \in S_n^\wedge$. It follows that the GZ-vectors are the only vectors that are eigenvectors for the action of every element of GZ_n . Moreover, any GZ-vector is uniquely determined by the eigenvalues of the elements of GZ_n on this vector.

(C) For $i = 1, 2, \dots, n$ define $X_i = (1, i) + (2, i) + \dots + (i-1, i) \in \mathbb{C}[S_n]$. The X_i 's are called the Young-Jucys-Murphy elements (YJM-elements) and it is shown that they generate GZ_n . To a GZ-vector v we associate the tuple $\alpha(v) = (a_1, a_2, \dots, a_n)$, where $a_i =$ eigenvalue of X_i on v . We call $\alpha(v)$ the *weight* of v and we set

$$\text{spec}(n) = \{\alpha(v) : v \text{ is a GZ-vector}\}.$$

It follows from step (B) above that, for GZ-vectors u and v , $u = v$ iff $\alpha(u) = \alpha(v)$ and thus $\#\text{spec}(n) = \sum_{\lambda \in S_n^\wedge} \dim L^\lambda$. Given $\alpha \in \text{spec}(n)$ we denote by v_α ($\in L^\lambda$ for some unique $\lambda \in S_n^\wedge$) the GZ-vector with weight α .

There is a natural equivalence relation \sim on $\text{spec}(n)$: for $\alpha, \beta \in \text{spec}(n)$,

$$\alpha \sim \beta \iff v_\alpha \text{ and } v_\beta \text{ belong to the same irreducible } S_n\text{-module } L^\lambda \text{ for some } \lambda \in S_n^\wedge$$

Clearly we have $\#(\text{spec}(n)/\sim) = \#S_n^\wedge =$ number of partitions of n .

(D) In the final step we construct a bijection between $\text{spec}(n)$ and $\text{tab}(n)$ (= set of all standard Young tableaux on the letters $\{1, 2, \dots, n\}$) sending weights in $\text{spec}(n)$ to content vectors of standard Young tableaux showing, in particular, that the weights are integral. Weights in $\text{spec}(n)$ that are related by \sim go to standard Young tableaux of the same shape. We shall not use this step.

Let V be a S_n -module, not necessarily multiplicity free. For $\alpha = (a_1, a_2, \dots, a_n) \in \text{spec}(n)$ define the *weight space*

$$V(\alpha) = \{v \in V : X_i(v) = a_i v, \ i = 1, \dots, n\}.$$

Note that, if V is multiplicity free, then it follows from items (B), (C) above that every weight space is either zero or one dimensional.

For $\lambda \in S_n^\wedge$, let $V(\lambda) \subseteq V$ denote the isotypical component of L^λ and let $\text{spec}(n, \lambda)$ denote the set of all weights $\alpha \in \text{spec}(n)$ with $v_\alpha \in L^\lambda$. Basic properties of the weight spaces are given below.

Lemma 4.1 *Let V, W be S_n -modules. We have*

(i) *For $\lambda \in S_n^\wedge$, $V(\lambda) = \bigoplus_{\alpha \in \text{spec}(n, \lambda)} V(\alpha)$ is an orthogonal decomposition of $V(\lambda)$ under any S_n -invariant inner product on V .*

(ii) *$V = \bigoplus_{\alpha \in \text{spec}(n)} V(\alpha)$ is an orthogonal decomposition of V under any S_n -invariant inner product on V .*

(iii) *Let $\lambda \in S_n^\wedge$, and $\alpha, \beta \in \text{spec}(n, \lambda)$. There is a canonical linear isomorphism $f_{\alpha, \beta} : V(\alpha) \rightarrow V(\beta)$, unique upto scalars, satisfying the following property: for $v \in V(\alpha)$, the subspace $\mathbb{C}[S_n]v \cap V(\beta)$ is generated by $f_{\alpha, \beta}(v)$.*

(iv) *Let $\lambda \in S_n^\wedge$, $\alpha \in \text{spec}(n, \lambda)$, and $f : V(\lambda) \rightarrow W(\lambda)$ a S_n -linear map. Then $f(V(\alpha)) \subseteq W(\alpha)$ and any linear map $g : V(\alpha) \rightarrow W(\alpha)$ has a unique S_n -linear extension $g : V(\lambda) \rightarrow W(\lambda)$.*

Proof (i) Fix a S_n -invariant inner product on V and let $V(\lambda) = W_1 \oplus \dots \oplus W_t$ be an orthogonal decomposition of $V(\lambda)$ into irreducible submodules, with all W_i isomorphic to L^λ . For $\alpha \in \text{spec}(n, \lambda)$ it follows from (B), (C) above that $V(\alpha) \cap W_i$ is one dimensional for all i and that the span of these one dimensional subspaces is $V(\alpha)$. Since the GZ-bases of W_i are orthogonal the result follows.

(ii) Follows from part (i), since the decomposition of V into isotypical components is orthogonal.

(iii) Let $v \in V(\alpha)$. Consider the irreducible submodule $\mathbb{C}[S_n]v$ of V generated by v . By item (B) above the subspace $\mathbb{C}[S_n]v \cap V(\beta)$ is one dimensional, say generated by u . There is an element $a \in \mathbb{C}[S_n]$ with $av = u$. The linear map

$$V(\alpha) \rightarrow V(\beta), \ x \mapsto ax \tag{38}$$

has the required properties. It is also clear that such a map is unique upto scalars.

(iv) The first part of the assertion is clear. For the second part note that (38) implies that g has atmost one S_n -linear extension. Dimension considerations now show that g has exactly one S_n -linear extension. \square

Consider the poset $M(n, k)$, on which the symmetric group S_n acts by substitution. Set $V = V(M(n, k))$ and $V_i = V(M(n, k)_i)$, $0 \leq i \leq kn$. Note that each V_i is a S_n -submodule of V and, for $\alpha \in \text{spec}(n)$, we have $V(\alpha) = V_0(\alpha) \oplus \dots \oplus V_{kn}(\alpha)$. Since the up operator U is S_n -linear it follows from Lemma 4.1(iv) that

$$U(V_i(\alpha)) \subseteq V_{i+1}(\alpha), \ 0 \leq i < kn, \ \alpha \in \text{spec}(n). \tag{39}$$

Let $C = (v_i, v_{i+1}, \dots, v_{kn-i})$, with $r(v_l) = l$ for all l , be a symmetric Jordan chain in V . We say that C is a *symmetric Gelfand-Tsetlin chain* if each v_l is a simultaneous eigenvector for the action of X_1, X_2, \dots, X_n . It follows that $v_l \in V_l(\alpha)$, $i \leq l \leq kn - i$, for some $\alpha \in \text{spec}(n)$. Since an SJB of V exists, it follows from Lemma 4.1(ii) and (39) that there exists a SJB of V consisting of symmetric Gelfand-Tsetlin chains. However, in such a SJB the Gelfand-Tsetlin chains belonging to different weight spaces (of the same isotypical component) need not be related to each other. Note that, for $\alpha \sim \beta$, $\alpha, \beta \in \text{spec}(n)$, if C is a Gelfand-Tsetlin chain in $V(\alpha)$ then $f_{\alpha, \beta}(C)$ is a Gelfand-Tsetlin chain in $V(\beta)$ (from (38) and the fact that U is S_n -linear). We now add this condition to the definition.

A *symmetric Gelfand-Tsetlin basis* (SGZB) of V is a SJB B of V satisfying the following conditions:

- (a) Each vector in B is a simultaneous eigenvector for the action of X_1, \dots, X_n .
- (b) For $\alpha \sim \beta$, $\alpha, \beta \in \text{spec}(n)$, if $v \in B \cap V(\alpha)$, then some multiple of $f_{\alpha, \beta}(v)$ is also in B .

Clearly, a SGZB of V exists (for each isotypical component choose a SJB of any one weight space and transfer it to the other weight spaces via $f_{\alpha, \beta}$). In the special case of Boolean algebras this definition of SGZB coincides with the one given in the introduction (see proof of Theorem 1.3 below).

At this point two natural questions arise:

- (i) Is it possible to characterize in some way the SJB produced by the linear BTK algorithm?
- (ii) Is there an explicit construction (inductive or direct) of a SGZB of $V(M(n, k))$?

Theorem 1.3 answers both these questions in the special case of Boolean algebras. We now prove this result.

Lemma 4.2 *For $0 \leq i \leq n$, $V(B(n)_i)$ is a multiplicity free S_n -module with $\min\{i, n - i\} + 1$ irreducible summands.*

For the proof of this lemma see Theorem 29.13 in [JL]. To actually identify the irreducibles (as corresponding to two part partitions) see Example 7.18.8 in [S1]. To identify the irreducibles, along with their multiplicity (given by the number of semistandard Young tableaux), in the S_n -module $V(M(n, k)_i)$ see Exercise 7.75 in [S1].

Proof of Theorem 1.3 We shall show inductively that each element of $O(n)$ is a simultaneous eigenvector of X_1, \dots, X_n , the case $n = 1$ being clear. By Lemma 4.2, condition (b) in the definition of SGZB is then automatically satisfied. It also follows from Lemma 4.2 that in the case of $V(B(n))$ the definition of SGZB given in the introduction agrees with the definition given above.

Assume that each element of $O(n)$ is an eigenvector for the action of X_1, \dots, X_n . Note that if $v \in V(B(n)_k)$ is an eigenvector for X_i , for some $1 \leq i \leq n$, then $\bar{v} \in V(B(n+1)_{k+1})$ is also an eigenvector for X_i with the same eigenvalue. Thus it follows from (31, 33, 34, 35, 36) that each element of $O(n+1)$ is an eigenvector for X_1, \dots, X_n . It remains to show that each element of $O(n+1)$ is an eigenvector for X_{n+1} .

For $0 \leq i \leq \frac{n+1}{2}$ and $0 \leq k \leq i$ define a subset $R(k, i) \subseteq O(n+1)$ consisting of all $v \in O(n+1)$ satisfying: $r(v) = i$ and the symmetric Jordan chain in which v lies starts at rank k and ends at rank $n+1-k$. Put $W(k, i) = \text{Span } R(k, i)$. Clearly $V(B(n+1)_i) = W(0, i) \oplus W(1, i) \oplus \cdots \oplus W(i, i)$. We claim that each $W(k, i)$ is a S_{n+1} -submodule. We prove this by induction on i , the case $W(0, 0)$ being clear. Assume inductively that $W(0, i-1), \dots, W(i-1, i-1)$ are submodules, where $i \leq \frac{n+1}{2}$. Since U is S_{n+1} -linear, $U(W(j, i-1)) = W(j, i)$, $0 \leq j \leq i-1$ are submodules. Now consider $W(i, i)$. Let $u \in W(i, i)$ and $\pi \in S_{n+1}$. Since U is S_{n+1} -linear we have $U^{n+2-2i}(\pi u) = \pi U^{n+2-2i}(u) = 0$. It follows that $\pi u \in W(i, i)$.

We now have from Lemma 4.2 that, for $0 \leq i \leq \frac{n+1}{2}$, $W(0, i), \dots, W(i, i)$ are mutually non-isomorphic irreducibles. Consider the S_{n+1} -linear map $f : V(B(n+1)_i) \rightarrow V(B(n+1)_i)$ given by $f(v) = av$, where

$$a = \text{sum of all transpositions in } S_{n+1} = X_1 + \cdots + X_{n+1}.$$

It follows by Schur's lemma that there exist scalars $\lambda_0, \dots, \lambda_i$ such that $f(u) = \lambda_k u$, for $u \in W(k, i)$. Thus each element of $R(k, i)$ is an eigenvector for $X_1 + \cdots + X_{n+1}$ (and also for X_1, \dots, X_n). It follows that each element of $R(k, i)$ is an eigenvector for X_{n+1} .

The paragraph above has shown that the bottom element of each symmetric Jordan chain in $O(n+1)$ is a simultaneous eigenvector for X_1, \dots, X_{n+1} . It now follows from Lemma 4.1(iv) that each element of $O(n+1)$ is a simultaneous eigenvector for X_1, \dots, X_{n+1} . That completes the proof. \square

Acknowledgement

I am grateful to Sivaramakrishnan Sivasubramanian for several helpful discussions and to Professor Alexander Schrijver for an encouraging e-mail.

References

- [A] I. Anderson, *Combinatorics of finite sets*, Clarendon Press, Oxford, 1987.
- [BTK] N. G. de Bruijn, C. A. v. E. Tengbergen and D. Kruyswijk, *On the set of divisors of a number*, Nieuw Arch. Wiskunde, 23: 191-193 (1951).
- [C] E. R. Canfield, *A Sperner property preserved by product*, Linear and Multilinear Algebra, 9: 151-157 (1980).
- [E] K. Engel, *Sperner theory*, Cambridge University Press, 1997.
- [D1] C. F. Dunkl, *A Krawtchouk polynomial addition theorem and wreath product of symmetric groups*, Indiana University Mathematics Journal, 26: 335-358 (1976).
- [D2] C. F. Dunkl, *Spherical functions on compact groups and applications to special functions*, Symposia Mathematica, 22: 145-161, Academic Press, London - 1977.

- [GST] D. Gijswijt, A. Schrijver, and H. Tanaka, *New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming*, Journal of Combinatorial Theory, Series A, 113: 1719-1731 (2006).
- [GW] R. Goodman, and N. R. Wallach, Symmetry, Representations, and Invariants, *Graduate Texts in Mathematics*, Springer, 2009.
- [JL] G. James, and M. Liebeck, Representations and Characters of Groups, *Cambridge University Press*, 2001.
- [P] R. A. Proctor, *Representations of $sl(2, \mathbb{C})$ on posets and the Sperner property*, SIAM Journal of Algebraic and Discrete Methods, 3:275-280 (1982).
- [PSS] R. A. Proctor, M. E. Saks and P. G. Sturtevant, *Product partial orders with the Sperner property*, Discrete Mathematics, 30: 173-180 (1980).
- [S] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Transactions on Information Theory, 51: 2859-2866 (2005).
- [S1] R. P. Stanley, Enumerative Combinatorics - Volume 2, *Cambridge University Press*, 1999.
- [V] F. Vallentin, *Symmetry in semidefinite programs*, Linear Algebra and its Applications, 430: 360-369 (2009).
- [VO] A. M. Vershik and A. Okounkov, *A new approach to the representation theory of the symmetric groups - II*, Journal of Mathematical Sciences (New York), 131: 5471-5494 (2005).